Risk communication within military decision-making: pedagogic considerations

Risk management is a decision-support process and a vital tool for military planning and decision-making. Today, several nations utilize risk-based approaches to analyze the level of security in military operations. There are both strengths and challenges in applying risk-based approaches to support military decisions. In this article, the challenges related to risk communication are investigated with the aim of describing how a military organization should train to create a good environment for effective risk communication. The analysis finds that it is important for the organization to define and consistently use a shared risk understanding. Such a shared risk understanding will need a systematic development process that focuses on the future decision makers' and analysts' education and training. To reach understanding, all involved parties must have the chance to identify the problem, reflect on its implications, test different solutions and develop a solution.

Keywords: risk communication; pedagogic considerations; military decision-making; risk management; uncertainties; risk understanding

Introduction

Today, several nations and organizations employ risk-based approaches to analyze the level of security in military operations [1-6]. There are strengths to applying risk-based approaches to support military decisions, but there are also challenges [7]. Many of these challenges are not recognized in doctrines or handbooks [8]. For civilian risk-based approaches, important discussions exist on the strengths and weaknesses of approaches and tools, such as Aven and Krohn [9]; Frosdick [10]; Hansson [11]; Hubbard [12]; and Kunreuther [13] and on the challenges in risk communication [14, 15]. However, the discussions on problems or limitations with military approaches are few.

From experience with civilian risk-based approaches, it is clear that the safety culture in general will affect both risk management and risk communication. Relative to the challenges that military personnel face when considering different types of operations in different settings, the variability in aim and values in civilian industry are often straightforward. For example, a military unit often trains for both warfighting and peace-keeping, two activities that require completely different cultures and risk understanding [16, 17]. Therefore, there are substantial challenges for risk communication within a military context relative to the organizational culture.

Both the areas presented above and previous research [18] show that the challenge for military organizations in relation to risk management is a challenge on how the risk understanding should be related to the specific organization's tasks and context. Although the traditional pedagogic view on risk communication, in which the receiver must be taught "the right risk understanding", has been abandoned, there are still important pedagogic aspects of risk communication to investigate, especially in inter-organization communication. The aim of this study is to increase the understanding of risk communication in the military context and to describe how a military organization should train to create a good environment for effective risk communication. Therefore, this study analyzes military risk and risk communication in relation to ontology, epistemology, communication and leadership to identify central pedagogical aspects of risk communication so these aspects can be implemented in military education and training. The study focus on the needs presented by communicating the risk analysis results to a military decision maker. However, other types of military risk communication are also touched on in the discussion.

Initially, in the theory section, the central theoretical concepts (epistemology, communication, leadership and understanding) are briefly defined. Thereafter, the section on risk communication and risk management in military organizations first introduces risk management in general and then describes the two central areas for analysis: risk communication and risk management in military organizations. In the analysis section, risk communication and risk management in military organizations are analyzed in relation to the concepts described in the theory section.

Theory

The concepts described below are assumed to be well known. Therefore, the descriptions below only briefly introduce them and then focus on defining how they are used in this study.

Epistemology

Epistemology is the theory of knowledge, whose central question includes the origin of knowledge; ontology concerns itself with what exists and addresses questions concerning what entities exist and how existence can be understood or rationalized [19]. The concepts within epistemology, such as the changing forms of knowledge that arise from new conceptualizations of the world, link to other central concerns of philosophy such as ontology. Therefore, epistemology is the branch of philosophy that is concerned with the nature and scope of knowledge; it is also referred to as the "theory of knowledge." It questions what knowledge is and how it can be acquired. The basic epistemological questions about knowledge, such as "What is knowledge?", can also be asked about risk and are herein used to identify epistemological challenges within military risk communication.

Communication and leadership

Communication is the transmission of information. Problems within the philosophy of communication include the question of whether communication is essential to thought and whether we can do better than thinking of words as mere vehicles for independent thoughts or ideas [19]. All communications are performed in a context and must be analyzed and understood based on that context. The context can be divided into a physical context, an emotional context and a cultural context. Our understanding of this context and the person with whom we are communicating are often formulated too rapidly based on easy-to-identify cues such as clothes [20]. In this study, there is no substantial difference between the term communication and the term knowledge-sharing, which also has strong cultural ties [21].

A way of understanding how a person is interacting with others is the Johari window. The theory, created by Joseph Luft and Harrington Ingham in the mid-1950s divides the understanding of ourselves into four windows. Window one is the part of ourselves that we see and others see. Window two is the aspects that others see but we are not aware of. Window three is the things that we know but keep from others, and finally, window four is the most mysterious room in that it is the unconscious or subconscious part of us that is seen by neither ourselves nor others. [20]

The term leadership has different definitions depending on the perspective of the user of the term. However, most definitions reflect the assumption that it involves a process in which a person uses intentional influence to guide, structure or facilitate activities in an organization [22]. In this study, leadership is viewed as an activity that is performed by a specific person with the role of making decisions within the organization, i.e., leadership is herein considered to be performed by the decision maker.

Despite the many different possible definitions of leadership, most behavioral scientists and practitioners believe that how leadership is performed is important for the effectiveness of the organization [22]. However, the decisions made by leaders are seldom fully structured, and choosing among unattractive alternatives is often accompanied by several negative feelings that can affect the decisions made [23].

It is common practice within a decision setting to consult with subordinates, peers or superiors. However, the different people involved in a decision often disagree on the nature of the problem as well as on the solutions [23].

Understanding in a pedagogic context

Understanding in a pedagogic context here relates to deep learning, and to do that, students must do more than just listen to be engaged in the process. "Most important, to be actively involved, students mast engage in such higher-order thinking tasks as analysis, synthesis, and evaluation" [24]. When an individual experiences something, for example, that something is not right, will that individual try to understand the problem with the help of her mind or act immediately and, with trial and error, find a solution? This means that we can work with the experience either intellectually or in practice. Both processes lead to understanding. Therefore, the process for creating understanding starts when a person (i) *identifies a problem* and thereafter works with that problem both (ii) *in the mind* and through (iii) *experimentation* and then (iv) *formulates an answer* [25]. Over time, all four of these aspects are needed to create an understanding, as well as to create qualitative training [26].

Subsequently, a suitable learning process that facilitates the participants' understanding of the questions at hand is needed to activate the participants in the four aspects described above. The learning activities must therefore support such activities.

Risk communication and risk management in military organizations

Risk management in general

Risk management is a decision-support process, and the risk analysis itself is a vital tool for military planning and decision-making [2, 27]. Risk management have been utilized since the 1950s to control hazards in areas such as industrial plants and space travel [28]. The use of risk management tools in decision-making is growing and is expected to grow further [15].

Risk management is herein defined as the systematic application of management policies, procedures and practices to the task of analyzing, evaluating and controlling risk (Figure 1).

Risk or risk level is defined as a function of the probability of the occurrence of an unexpected/unwanted event and the consequence of it occurring. Risk communication is important in all activities of a risk management process. However, it is crucial in the risk evaluation because the risk is most often analyzed by the analysts and the decisions made by the decision maker.

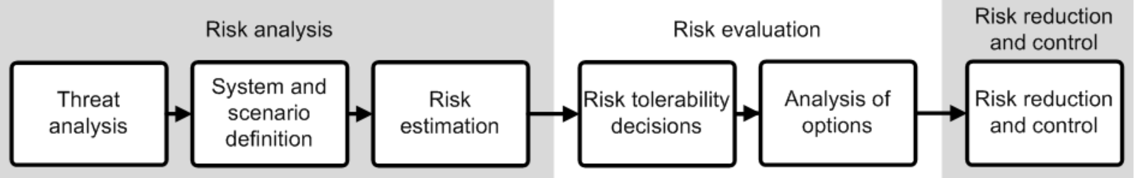
Risk analysis
Threat analysis
System and scenario definition
Risk estimation
Risk evaluation
Risk tolerability decisions
Analysis of options
Risk reduction and control
Risk reduction and control

Figure 1. The security risk management process and its components developed from Liwång, Ericson [8].

The results of a risk analysis must always be weighed against both risk tolerability levels and other operational parameters, such as possible operational gain, requested reliability and financial considerations. Generally, higher risks are tolerable if the possible operational gain is high [2, 5, 29, 30].

The traditional engineering approach to risk analysis is based on objectivist expected utility, which combines objectivist probabilities with objectivist utilities. This means that the concept of probability that is used is interpreted as an objective representation of the frequency of the studied event with a linear relationship between the consequences studied and their utility assignments [11], e.g., a solution with consequences that are twice as high but have the same probability is twice as bad. However, there has been development towards a system perspective on safety that includes not only technology and structure but also, and just as importantly, processes and social systems [31]. This new view broadens the scope of risk management.

In general, probabilistic risk assessments offer a sound and systematic basis for evaluating potentially hazardous activity. However, the methods used are specialized and often complex, and it is important to ensure a logical and consistent approach and that relevant data have been adopted. [28]

Risk communication

Risk communication combines social communication, practical management and policy-making [14] and requires an understanding of the concept of both risk and uncertainties [32]. Risk communication "involves several distinctions, including that between expert and laymen, between those affected by decision and those who make the decisions, between conflict and co-operation, between facts and values, and between inclusion and exclusion in decision processes" [14]. Therefore, risk communication was initially discussed in a pedagogical setting where the mission was to teach the public about "real risk" so they can make rational choices about what risks to take [14]. However, the emphasis has now shifted from education to a mutual understanding [14]. This is further highlighted by a need to view risk management as an iterative process, not a final answer [15] in a system perspective [31]. This has also changed the paradigm from a technological sender-receiver model to a dialog model. It has been shown that communication failure occurs when the understanding of the message at the receiver's end differs significantly from the message intended from the sender [14]. However, at the same time, we cannot oversimplify the risk message because simplifications such as using a point estimate may ignore important underlying dynamics [15]. Including uncertainty in the analysis and disclosing the output uncertainty in the results includes more knowledge into the analysis but can, at the same time, be perceived as a weakness [15].

Means such as dialogue, different viewpoints, evaluations and prioritizations will facilitate decision-making on collective and often controversial matters that are imbued with risk and uncertainty. "Trust between participants is a crucial condition for dialogue" [14]. If persons are to be involved constructively in decision-making based on risk assessment, they need to be able to understand the magnitude of the risk. Without quantitative risk information, the persons involved will resort to traditional gut feelings that are "influenced by past experiences, affect and emotion, the views of acquaintances, and cultural beliefs" for making risk management decisions. Quantitative risk communication is an imperative, however, not only to improve decision-making but also to support democratic processes [32]. Further, performing a proper uncertainty and/or sensitivity analysis is crucial to capture how changes affect the risk [15].

Research has indicated that the most important basic knowledge type that is crucial for understanding risk communication is general math understanding (numeracy). In a study on risk communication about unexploded ordnance [32], it was found that the participant's general math knowledge significantly increased understanding of mean risk and uncertainty, decision-making and perceived risk. The study on unexploded ordnance risk also highlighted the need to develop more effective means of communicating uncertainty information. In particular, graphical approaches that have proven useful in communicating central risk estimates may be ineffective for communicating uncertainty. Therefore, the authors concluded that future research should be directed toward developing new techniques for communicating uncertainty information. [32]

Risk decisions in a military context

Casualties, whether deliberate or accidental, are a reality of military operations, and the desire to fully avoid them may have an adverse impact on the achievement of the mission. A balance of risk is therefore required, and risk management is often translated into operational procedures [18]. In military activity, risk must be understood in the broad socio-technical context [31]. For example, does Force protection require risk management and prioritization, including an integrated threat, vulnerability and risk analysis. This comprehensive risk assessment process is essential to guide risk management decision-making and prioritization [2, 5].

It is important to note that negative outcomes and their probability (risk) as well as positive outcomes and their probability (expected gain) must be estimated and assessed. Risk can therefore only provide part of the picture needed for making a decision. In general, military decision-making must be understood within a system-thinking perspective [33]. Therefore, risk analysis must be an integral part of the decision analysis and cannot be separated, in time or space or organizationally, from the decision-making process in general [34].

It is worth noting that the military applications of risk management have great similarities with their civilian predecessors, though the civilian approaches are mainly developed for safety, whereas military applications are often about security where the uncertainties generally are high [9].

An example where the importance of uncertainties in security assessment is discussed is the US Presidential Policy Directive for critical infrastructure, security and resilience [35], which promotes resilience. Resilience is achieved with robust control options or generic capabilities, which are less sensitive to uncertainties [36]. These aspects can only be studied if the uncertainties are included throughout the risk analysis.

One example of such uncertainty is the disagreement among security experts about Osama bin Laden's hiding place, as described by Friedman and Zeckhauser [37]. However, despite the relatively substantial uncertainty, the US President had to make a decision about the next step of the operation. This example provides a good description of the setting for security risk management:

- There are substantial epistemic uncertainties in a security analysis, but
- despite those uncertainties, decisions must be made.

Liwång, Ericson [8] identified that the risk assumptions for military risk are not explicitly stated in the doctrines, and both Liwång [34] and Bakx and Nyce [31] show that the concept of risk in the military context cannot be fully objectivistic. This means that risk as a concept in military as well as other security settings has several subjective aspects and that a correct risk estimate does not exist [31, 38].

The lack of a specific discussion on how to understand risk and the resulting choices of risk analysis tools and how these choices affects the output in the doctrines is problematic [18]. This problem may also be increased as a result of varying tasks, different nations' organizational culture and the fact that the organization solving the task is occasionally temporally formed from different organizational entities [16, 17, 21].

Therefore, security risk management, as seen above, presents specific challenges. Three of these – (1) shared risk awareness, (2) system/scenario definition, and (3) risk perception and cultural bias – are briefly described below and are then revisited when the pedagogic implications are described.

(1) Shared risk awareness is needed throughout the organization and can only exist if the risk and uncertainty are assessed in a documented, structured and standardized manner [8, 34] that aligns with the organizations decision-making and used decision-support activities. This is especially challenging in military organizations as the culture, approach to decision-making and operational context vary among operations, organizations and nations [18].

(2) The system and scenario definition is a central task of the risk analysis and will affect every aspect of the risk estimation. Two challenging aspects of the definition are the timespan and the consequences to study; there is no discussion on that aspect in the doctrines studied here [8, 34]. There must be different system definitions for different decision-making situations. Otherwise, the scenario cannot be finite. This understanding must be implemented throughout the organization, and the principles for system definition must be communicated and continuously updated. If different principles for system definition exist side by side within an organization, the basis for decision-making will be unbalanced, which may lead to decisions not using the actual knowledge at hand [34] .

(3) Risk perception and cultural bias has shown to be weak in risk management in general [10]. The reasoning in military organizations with respect to risk rationality may

differ at different hierarchy levels [3, 18]. Therefore, an effective application of risk analysis places non-trivial responsibilities on the analyst and the decision maker. The analyst must also be responsible for documenting and describing all consequences separately as well as the limitations resulting from the chosen system definition. The decision maker then has the responsibility to weigh different consequences against each other. This also leads to a need for the decision maker to be involved in system definition and the definition of the consequences under study [34]. The risk management starts with the decision maker asking for the appropriate analysis.

Analysis

Using the areas presented in previous sections, this section analyzes risk and risk communication within military organizations in relation to ontology, epistemology, communication and leadership to identify central pedagogical aspects of military risk communication.

Epistemology: what is military risk, and how can a military organization know risk?

The basic epistemological questions about knowledge can also be asked about risk: "What is risk?", "How is risk knowledge acquired?", "What do people know about risk?", and "What are the necessary and sufficient conditions of risk knowledge?”.

From an epistemological perspective, risk can be viewed as (new) conceptualizations of the world. When talking about risk as a result of the failure of a simple technical system (such as of a set of pumps, valves and pipes, which is a typical situation for which risk analysis tools are developed), the risk can be truly concreate and measurable. By examining the system and its components and recording failure frequencies and consequences, the risk can be fully described and therefore measured without ambiguity and epistemic uncertainty. Therefore, the traditional engineering risk understanding is described as objectivistic. However, for military risk management, the engineering understanding is not suitable, and an alternative understanding is not presented in the doctrines. Therefore, the epistemological understanding of risk in a military context especially is not predefined. The understanding is not explicitly discussed and may therefore often vary between individuals and different hierarchy levels (see for example Turner and Tennant [18]).

The lack of a shared risk understanding will

- leave the selection of suitable methods and tools ungoverned,
- lead to challenges with respect to understanding the magnitude of the risk and which consequences to study,
- lead to challenges with respect to understanding what the epistemic uncertainty and variability mean in operational terms,
- not facilitate an informed discussion on how to develop resilient systems and generic capabilities, and
- not facilitate risk management as an iterative process where the analysis can easily be revisited in the future.

To be able to discuss risk, uncertainty and variability, acceptable levels of risk and the challenges of risk management, the civilian community has been developing and updating examples. Two such examples, as described by Thompson [15], are risk to groundlings from airplane crashes and the risk posed by airbags. Given the challenges identified here, it is likely that developing a set of military cases that illustrate and represent critical levels of risk but also include uncertainty and variability can support the development of a shared risk understanding. Other important aspect to military decisions that could be illustrated by such cases is that the acceptable risk levels vary with the type of operation, ranging from high acceptable risk in war and often lower acceptable risk in peacekeeping operations. The examples also should illustrate the links between how risk is defined, the consequences to study and the decisions made.

Military risk communication and leadership

Today, effective risk communication is often described as a dialog. It has been shown that communication failure occurs when the message at the receiver’s end differs significantly (is understood differently) from the message dispatched (or intended understanding) from the sender due to different risk understanding. To avoid such failure, there needs to be a dialog that is based on a mutual understanding that should not be oversimplified. Subsequently, it is also important that the decision maker’s risk understanding is explicit and understood by the risk analyst (the risk understanding has to exist in Johari window number one). Such a shared risk understanding can only be accomplished if risk and risk understanding are continuously discussed in a dialog climate among the involved personnel.

The decision context is often complex enough; for example, the different people involved in a decision often disagree on the nature of the problem and on the solutions, and people often tend to discount important and unexpected information because it does not fit into their assumptions on how things work. Therefore, the decision maker cannot afford to spend valuable time on coordinating the risk understanding, which must be developed as much as possible prior to making operational decisions. Subsequently, risk management, good leadership, sufficient communication skills and a holistic view are not sufficient; a suitable risk understanding must also be in place and cannot be developed without support from the decision maker. Based on the risk understanding, the risk management is initiated by the decision maker and starts with the decision maker asking for the appropriate analysis.

To avoid communication being governed by easy-to-identify cues (such as rank), the decision maker has to take charge over defining the communication context and the cultural climate for the sharing of information.

The demands on risk decision-making are high. This is a result of a complex risk management process that, to be effective, needs to address uncertainties and be an iterative process. The following aspects are of extra importance in a military setting:

- Typically, risk assessment is performed at several levels, with more detail on lower levels. Therefore, the approaches used, the documentation and the decisions made must be able to support decisions on higher levels. The iterative process must also allow for being updated if the assumptions made are affected by decisions on higher levels.
- The effect of the existing culture in relation to the organization's tasks because the existing culture may be inadequate for dealing with the tasks at hand, i.e., fruitful risk understanding is often far from constant.
- "Risk assessment is a process for summarizing the available … information in both qualitative and quantitative form" [39], for decision makers. Thus, decisions should be driven by a comprehensive characterization of available information, including uncertainties. See NRC [39] for a detailed discussion for a civilian application.

Pedagogic implications

As described above, risk management is a powerful tool used in many settings, but it requires an understood and shared definition of risk and of the role of the risk management in relation to the decision-making process and the operation in general. It must be assumed that it is possible for a military organization to create a shared risk understanding by performing education and training for the involved personnel. This education and training cannot limit itself to merely describing the form of the risk management process. All involved parties must have the chance to identify the problem, reflect on its implications, test different solutions and develop a solution.

The methods used within a risk analysis are specialized and often complex and it is vital to ensure a well implemented approach. Therefore, the risk management education and training cannot be oversimplified. The education and training should support a dialog model.

(1) Shared risk awareness is key. To be able to discuss risk, uncertainty and variability, the acceptable level of risk and the challenges of risk management, the civilian community has been developing and updating examples. Given the challenges identified here, it is likely that education and training would benefit from developing a set of military cases that illustrate and represent critical levels of risk but also include uncertainty and variability. Another important aspect to military decisions in such cases is that the acceptable risk levels vary with the type of operation, ranging from high acceptable risk in war and often lower acceptable risk in peacekeeping operations. In military risk, there is also an interaction among how risk is defined, what consequences are studied and what decisions are made.

This study has shown that the organization's risk understanding is central and not the exact process of the organizations’ risk management and analysts’ risk analysis. The processes should, however, reflect the risk understanding of the organization. The risk understanding of the organization will, for example, govern which consequences to study and subsequently, at least in part, affect the selection of tools.

It is therefore important for the organization to define and consistently use a shared risk understanding. Such a shared risk understanding will not emerge by itself; it will need a systematic development process that focuses on the future decision makers and analysts in education and training.

(2) System and scenario definition represents a more process-orientated risk assessment challenge but will affect every aspect of the risk estimation. However, defining and understanding the appropriate events, systems and scenarios to study in the risk analysis can only be achieved as a result of a shared risk awareness. To perform manageable analysis, there must be different system definitions for different decision-making instances. The simplifications that can be used will vary across decision types, operation types and operational settings. Therefore, a shared risk understanding is not sufficient; it must, for example, be accompanied by an understanding on how the risk decisions will change when decision settings go from peacetime to war. This understanding must be implemented throughout the organization. For example, if different principles for system definition exist side by side within an organization, the basis for decision-making will be unknown, which may lead to decisions that do not use the actual knowledge at hand.

(3) Risk perception and cultural bias often affect the decision setting itself if the persons judge the communication based on easy-to-identify cues rather than listening to

what is said. Therefore, the decision maker has to take charge of the overall decision setting long before the decisions take place, i.e., in education and training, defining the communication context and the cultural climate for the sharing of information.

However, risk perception and cultural bias also affect the risk assessment. Therefore, education should support the aim of creating an iterative view on risk management, which needs an openness and a structured process that are today often contradicted by the secretive approach to security analysis.

Including uncertainty in the analysis and disclosing the output uncertainty in the results includes more knowledge in the analysis but can be perceived as a weakness of the analysis. Therefore, trust is important and must be built and maintained between analysts and decision makers.

Summarizing the analysis. It has been identified that organizations' risk understanding is central and is not the exact process of the organizations' risk management and the analysts' risk analysis. Educational and training efforts for the personnel involved in the risk management process must therefore focus on the abstract and philosophical aspects of risk rather than on the process of risk management itself. The processes should, however, reflect the risk understanding used in the organization. The risk understanding of the organization will, for example, govern which consequences to study. Identifying these consequences will at least in part affect the tool selection.

It is therefore important for the organization to define and consistently use a shared risk understanding, especially in the activities leading up to the real decision setting. Such a shared risk understanding will not emerge by itself; it will need a systematic development process and education and training that is focused on future decision makers and analysts. Civilian work has shown that using well-developed examples that include relevant risk levels, uncertainty and variability are effective to achieve this.

This education and training cannot be limited to merely describing a form of the risk management process. To reach understanding, all involved parties must have the chance to identify the problem, reflect on its implications, test different solutions and develop a solution. The risk understanding must also, in both education and training, be tested and discussed within different decision settings, such as for risk management in peacekeeping operations and in war. An organization will only be ready for risk management when the risk understanding is shared and the organization comprehends how the decision context affects the risk.

A notable challenge shown to be important is ensuring that the persons involved in risk management have a sufficient numeracy. In contradiction to a shared risk understanding, which should be developed with group education, training numeracy is developed in a more traditional educational setting and as a result of a personal education. For a military organization, this for example means that commanding personnel must be chosen carefully.

Discussion

The aim of this study is to increase the understanding of military decision-making in relation to risk communication. This especially done to describe how a military organization should train for creating a good environment for effective risk communication.

The risk management doctrines are formative to their nature, but to a large extent they limit their formative aspects to the form of the risk management, i.e., a process description, and leave the risk understanding ungoverned. Here, it has been identified that many challenges relate to the risk understanding and how it is shared but also to whether it is dynamic. The understanding must be dynamic, but the form of the risk management must also be dynamic and able to change if the decision settings change.

This study has studied the inter-organizational aspects of risk between the analyst and the decision maker where all involved parties exist within the same organization. This means that all involved have a possibility to prepare. However, there is also a need for military organizations to perform risk communication to the public and from the decision maker to military personnel in general. In such cases, the pedagogic challenges are different. The relevant areas are most likely the same but cannot be overcome by preparing the different involved parties. For example, when communicating military risk to the public, the “risk communicator” must try to capture the risk understanding of the public and must adopt and perform a dialog. This creates even more challenging demands for a developed risk understanding and for the communicator to be able to articulate her understanding in the communication.

Both military personnel in general and the public need to make decisions from time to time in which risk information from military decision makers is a factor. If this information needs to be used constructively, the receiver of the risk information needs to be able to understand the magnitude of the risk. If the risk information is not precise or understood as such, the persons involved will resort to traditional gut feelings that are influenced by past experiences and emotion for making risk management decisions.

If the value of the risk information shall inform decisions, there is a need for the public, military personnel and decision makers to be accustomed to discussing risk. How this is achieved depends on how risk and risk information are perceived. In a regulatory prescriptive setting, the value and results of a risk assessment can be reduced to a number (risk estimate = consequence × probability) that is compared to an acceptable level of risk; if the risk is lower than the activity, a solution or an alternative is deemed as safe and can be used. However, in a dynamic setting, a risk assessment could and should be allowed to contribute holistically to understanding the decision context, i.e., the risk assessment is one way to explore the options and learn more about them. In such cases, the first of the aspects that should be included in the analysis and be involved in the assessment output is information about the uncertainties, which then also connects the output to the assumptions made and the system understanding used.

A more comprehensive approach on how to understand the contributions from risk management is also in line with scholars' descriptions of the "'New View' of safety, with its emphasis on whole systems and on the connection between the social and the artefactual" [31] as well as the need for "applying systems thinking on complex crisis situations to gain holistic understandings of the operational environments" [33]. It is also likely that an exploratory use of risk assessments will support the warfighter's ambitions to view risk management thinking as a "battle appreciation" (as described by Turner and Tennant [18]) rather than a constraint.

Conclusions

This study analyzed military risk and inter organization risk communication to identify central pedagogical aspects of risk communication so these aspects can be implemented in military education and training. The study has shown that the organization's risk understanding is central. The risk management processes selected should, however, reflect the risk understanding used in the organization. The risk understanding of the organization will, for example, govern which consequences are studied and will therefore guide the tool selection.

It is therefore important for the organization to define and consistently use a shared risk understanding. Such a shared risk understanding will need a systematic development process that focuses on education and training for the future decision makers and analysts. This education and training cannot limit itself to merely describing the form of the risk management process. To reach understanding, all involved parties must have the chance to identify the problem, reflect on its implications, test different solutions and develop a solution.

Civilian work has shown that using well-developed examples that include relevant risk levels, uncertainty and variability are effective to achieve this. The pedagogical considerations in relation to risk communication within military decision-making are thus a pedagogical challenge that is related more to philosophy and, in particular, epistemology than to the organizations' processes and tools.

References

1. Swedish Armed Forces, *Försvarsmaktens gemensamma riskhanteringsmodell [The Armed Forces joint risk management model]*. 2009, Stockholm: Swedish Armed Forces.

2. NATO, *Comprehensive operations planning directive, V1.0*, 2010, NATO Supreme Headquarters Allied Power Europe: Brussels.

3. Bakx, G.C.H. and R.A.L. Richardson, *Risk assessments at the Royal Netherlands Air Force: An explorative study.* Journal of Risk Research, 2013. **16**(5): p. 595-611.

4. Department of the Army, *Composite risk management, FM 5-19 (FM 100-14)*, 2006, Headquarters Department of the Army: Washington DC.

5. NATO, *Allied joint doctrine for force protection, AJP-3.14*, 2007, NATO Standardisation Agency: Brussels.

6. DCDC, *Joint force protection, Joint doctrine publication 3-64*, 2010, The Development, Concepts and Doctrine Centre, Ministry of Defence, United Kingdom: Shrivenham.

7. Tomes, S., *Risk: misunderstanding or military misnomer*, in *The British Army*

*Review*2012, Ministry of Defence: London. p. 32-40.

8. Liwång, H., M. Ericson, and M. Bang, *An examination of the implementation of risk based approaches in military operations.* Journal of Military Studies, 2014. **5**(2).

9. Aven, T. and B.S. Krohn, *A new perspective on how to understand, assess and manage risk and the unforeseen.* Reliability Engineering & System Safety, 2014. **121**(0): p. 1-10.

10. Frosdick, S., *The techniques of risk analysis are insufficient in themselves.* Disaster Prevention and Management, 1997. **6**(3): p. 165-177.

11. Hansson, S.O., *The false promise of risk analysis.* Ratio-New Series, 1993. **6**(1): p. 16-26.

12. Hubbard, D.W., *Worse than useless: The most popular risk assessment method and why it doesn't work*, in *The failure of risk management: Why it's broken and how to fix it*. 2009, John Wiley & Sons Inc.: Hoboken.

13. Kunreuther, H., *Risk analysis and risk management in an uncertain world.* Risk Analysis, 2002. **22**(4): p. 655-664.

14. Boholm, A., *New perspectives on risk communication: uncertainty in a complex society.* Journal of Risk Research, 2008. **11**(1-2): p. 1-3.

15. Thompson, K.M., *Variability and uncertainty meet risk management and risk communication.* Risk Analysis, 2002. **22**(3): p. 647-654.

16. Tardy, T., *The Reluctant Peacekeeper: France and the Use of Force in Peace Operations.* Journal of Strategic Studies, 2014. **37**(5): p. 770-792.

17. Moorkamp, M., et al., *Safety management theory and the expeditionary organization: A critical theoretical reflection.* Safety Science, 2014. **69**: p. 71-81.

18. Turner, N. and S.J. Tennant, *"As far as Is Reasonably Practicable": Socially Constructing Risk, Safety, and Accidents in Military Operations.* Journal of Business Ethics, 2010. **91**(1): p. 21-33.

19. Blackburn, S., in *The Oxford dictionary of philosophy*2008, Oxford University Press: Oxford.

20. Maltén, A., *Kommunikation och konflikthantering - en introduktion [Communication and conflict - an introduction]*. 1998, Lund: Studentlitteratur.

21. Friesl, M., S.A. Sackmann, and S. Kremser, *Knowledge sharing in new organizational entities The impact of hierarchy, organizational context, micro-politics and suspicion.* Cross Cultural Management-an International Journal, 2011. **18**(1): p. 71-86.

22. Yukl, G., *Introduction: The nature of leadership*, in *Leadership in organizations*. 2005, Pearson Education: Upper Saddle River. p. 1-21.

23. Yukl, G., *The nature of managerial work*, in *Leadership in organizations*. 2005, Pearson Education: Upper Saddle River. p. 22-49.

24. Bonwell, C.C. and J.A. Eison, *Active learning, creating excitement in the classroom*, ed. J.D. Fife. 1991, Washington DC: The George Washington University.

25. Kolb, D.A., *Experiential learning: experience as the source of learning and development*. 1984, Englewood Cliffs, NJ: Prentice Hall.

26. Döös, M., *Den kvalificerade erfarenheten. Lärande vid störningar i automatiserad produktion [The qualified experience. Learning when disturbances in automated production]*, in *Arbete och hälsa*1997, Arbetslivsinsitutet: Solna.

27. Johnson, C.W., *The paradoxes of military risk assessment*, in *the 25th International Systems Safety Conference*, A.G. Boyer and N.J. Gauthier, Editors. 2007, International Systems Safety Society: Baltimore, USA. p. 859-869.

28. Andrews, J.D. and T.R. Moss, *Risk assessment*, in *Reliability and risk assessment*. 2002, Professional Engineering Publishing Limited: London. p. 411-448.

29. IACS, *A Guide to Risk Assessment in Ship Operations*, 2012, International Association of Classification Societies: London.

30. IEC, *Dependability management - Application guide*, in *Section 9: Risk analysis of technological systems*1995, International Electromechanical Commission.

31. Bakx, G.C.H. and J.M. Nyce, *Risk and safety in large-scale socio-technological (military) systems: a literature review.* Journal of risk research, 2015.

32. Gibson, J.M., et al., *Communicating Quantitative Information About Unexploded Ordnance Risks to the Public.* Environmental Science & Technology, 2013. **47**(9): p. 4004-4013.

33. Lundqvist, S., *Why teaching comprehensive operations planning requires transformational learning.* Defence Studies, 2015. **15**(2): p. 175-201.

34. Liwång, H., *Risk-based ship security analysis – a decision-support approach*, in *Shipping and Marine Technology*2015, Chalmers University of Technology: Gothenburg. p. 73.

35. White House, *Presidential policy directive -- Critical infrastructure security and resilience*, 2013, The White House, Office of the Press Secretary: Washington DC.

36. Liwång, H., J.W. Ringsberg, and M. Norsell, *Quantitative risk analysis – Ship*

security analysis for effective risk control options. Safety Science, 2013. **58**: p. 98-112.

37. Friedman, J.A. and R. Zeckhauser, *Handling and Mishandling Estimative Probability: Likelihood, Confidence, and the Search for Bin Laden.* Intelligence and National Security, 2014: p. 1-23.

38. Aven, T., *On the allegations that small risks are treated out of proportion to their importance.* Reliability Engineering & System Safety, 2015. **140**(0): p. 116-121.

39. NRC, *Appendix N–2, Making full use of scientific information in risk assessment*, in *Science and Judgment in Risk Assessment*, National Research Council, Editor. 1994, National Academy Press: Washington D.C.